

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-229017

(43)Date of publication of application : 24.08.2001

(51)Int.Cl.

G06F 9/06
A61B 5/117
G06F 1/00

(21)Application number : 2000-036399

(71)Applicant : BASE TECHNOLOGY INC

(22)Date of filing : 15.02.2000

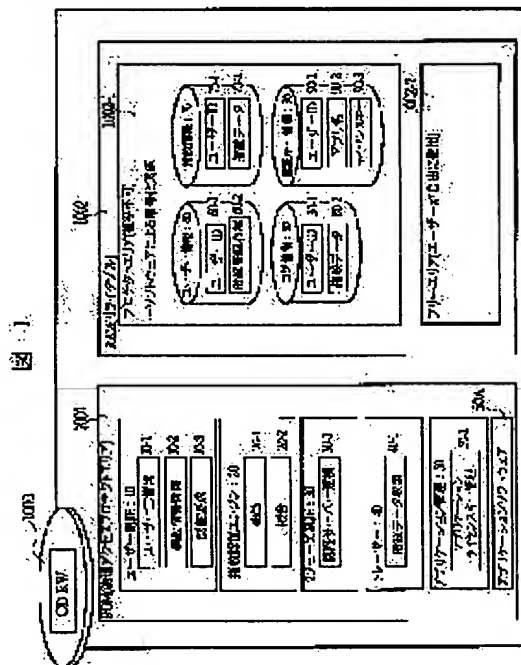
(72)Inventor : YAMANE SHIGEAKI
IMASHIRO TADAHIRO
YOSHIDA NAOKUNI

(54) PORTABLE RECORDING MEDIUM AND METHOD FOR USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To conveniently use various application softwares with high portability and security by using a portable recording medium.

SOLUTION: A CD-RW 1000 is provided with a read only physical access protect area 1001 and a rewritable area 1002, and plural application software 50A and a user authentication program 10 for executing user authentication by fingerprint collection and a fingerprint authentication engine 20 or the like are stored in the physical access protect area 1001, and fingerprint information 70 in which registered fingerprint data 70-2 and a corresponding user ID 70-1 are stored is stored in non-copying protect area 1002-1 if the rewritable area 1002. Thus, it is possible to complete the user authentication by the fingerprint collation and the use of the application software 50A after authentication in one CD-RW 1000.



LEGAL STATUS

[Date of request for examination] 15.02.2000

[Date of sending the examiner's decision of rejection] 26.11.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-229017

(P2001-229017A)

(43) 公開日 平成13年8月24日 (2001.8.24)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 G 4 C 0 3 8
A 6 1 B 5/117		1/00	3 7 0 E 5 B 0 7 6
G 0 6 F 1/00	3 7 0	A 6 1 B 5/10	3 2 0 A

審査請求 有 請求項の敬9 O L (全 11 頁)

(21) 出願番号 特願2000-36399 (P2000-36399)

(22) 出願日 平成12年2月15日 (2000.2.15)

(71) 出願人 397065952

ベーステクノロジー株式会社

東京都新宿区西新宿7-22-45

(72) 発明者 山根 茂昭

東京都新宿区西新宿7-22-45 ベーステクノロジー株式会社内

(72) 発明者 今城 忠浩

東京都新宿区西新宿7-22-45 ベーステクノロジー株式会社内

(74) 代理人 100080001

弁理士 筒井 大和 (外2名)

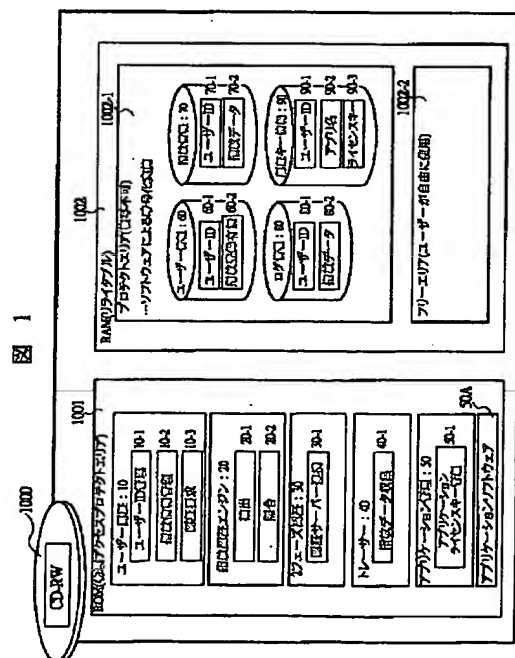
最終頁に続く

(54) 【発明の名称】 可搬性記録媒体および可搬性記録媒体の使用方法

(57) 【要約】

【課題】 可搬性記録媒体を用いて、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする。

【解決手段】 CD-RW1000に読み出し専用の物理アクセスプロテクトエリア1001と、書き換え可能なリライタブルエリア1002を設け、物理アクセスプロテクトエリア1001には、複数のアプリケーションソフトウェア50Aと、指紋照合によるユーザー認証を行うためのユーザー認証プログラム10、指紋認証エンジン20、等を格納し、リライタブルエリア1002の複写不可のプロテクトエリア1002-1には、登録された指紋データ70-2と、対応するユーザーID70-1が格納された指紋情報70を格納し、指紋照合によるユーザー認証、および認証後のアプリケーションソフトウェア50Aの利用が、一つのCD-RW1000内で完結するようにした。



【特許請求の範囲】

【請求項 1】 アプリケーションソフトウェアと、前記アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者による前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されていることを特徴とする可搬性記録媒体。

【請求項 2】 請求項 1 記載の可搬性記録媒体において、前記アプリケーションソフトウェアおよび前記認証ソフトウェアは、前記可搬性記録媒体の読み出し専用領域に格納され、前記個人識別情報は、前記可搬性記録媒体の書き換え可能領域に暗号化されて格納されていることを特徴とする可搬性記録媒体。

【請求項 3】 請求項 1 または 2 記載の可搬性記録媒体において、前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第 1 の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに依頼し、前記認証サーバーから照合結果を受け取ることで前記個人認証を行う第 2 の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体。

【請求項 4】 請求項 1、2 または 3 記載の可搬性記録媒体において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体。

【請求項 5】 アプリケーションソフトウェアが格納された可搬性記録媒体に、前記アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による前記可搬性記録媒体の前記アプリケーションソフトウェアの使用に先立って前記個人識別情報を用いた個人認証を行うことで、正当な前記利用者に、前記可搬性記録媒体に格納されている前記アプリケーションソフトウェアを使用させることを特徴とする可搬性記録媒体の使用法。

【請求項 6】 請求項 5 記載の可搬性記録媒体の使用法において、前記アプリケーションソフトウェアとともに前記可搬性記録媒体に格納されている認証ソフトウェアを用いて前記個人認証を行うことを特徴とする可搬性記録媒体の使用法。

【請求項 7】 請求項 6 記載の可搬性記録媒体の使用法において、前記アプリケーションソフトウェアとともに前記可搬性記録媒体に格納されている前記認証ソフトウェアは、前記可搬性記録媒体に格納されている前記個人識別情報と、任意の前記利用者が入力した個人識別情報を照合することで前記個人認証を行う第 1 の認証機能と、前記可搬性記録媒体に格納されている前記個人識別情報と任意の前記利用者が入力した個人識別情報との照合を、情報ネットワークを介して外部の認証サーバーに

依頼し、前記認証サーバーから照合結果を受け取ることと前記個人認証を行う第 2 の認証機能の少なくとも一方を含むことを特徴とする可搬性記録媒体の使用法。

【請求項 8】 請求項 7 記載の可搬性記録媒体の使用法において、前記認証サーバーは、複数の前記個人識別情報の各々と、個々の前記アプリケーションソフトウェアのライセンスキーとが対応付けて格納されたライセンスデータベースを持ち、前記個人識別情報に対応した前記ライセンスキーを前記照合結果として前記認証ソフトウェアの前記第 2 の認証機能に応答することで、前記可搬性記録媒体に格納された前記アプリケーションソフトウェアの利用機能の制限を行うことを特徴とする可搬性記録媒体の使用法。

【請求項 9】 請求項 5、6、7 または 8 記載の可搬性記録媒体の使用法において、前記個人識別情報は、前記利用者の指紋情報であることを特徴とする可搬性記録媒体の使用法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、可搬性記録媒体およびその使用技術に関し、特に、高度かつ多様なセキュリティ管理を必要とするアプリケーションソフトウェアが格納された可搬性記録媒体等に適用して有効な技術に関する。

【0002】

【従来の技術】たとえば、いわゆるインターネット等の情報ネットワークの発達および高性能のパーソナルコンピュータの広範な普及に伴い、パーソナルコンピュータを取り端末とする、電子商取引や、証券、金融サービスが普及してきている。

【0003】このようなパーソナルコンピュータを取り端末とする上述の各種サービスは、特定のパーソナルコンピュータに備えられた固定ディスク装置（HDD）等の外部記憶装置に当該サービス専用の端末ソフトウェア（アプリケーションソフトウェア）を実装して行われることが多い。

【0004】

【発明が解決しようとする課題】ところで、特定のパーソナルコンピュータに端末ソフトウェアを実装して利用する場合には、当該サービスの利用場所が特定のパーソナルコンピュータの設置場所に制約され、利用者にとって利便性に欠ける、という技術的課題がある。

【0005】さらに、実際のサービス利用に先立って、パーソナルコンピュータへのソフトウェアのインストール作業が必須となり、パーソナルコンピュータの知識に乏しい一般の利用者にとってはサービス利用の敷居が高くなり、サービス普及の障害となるとともに利便性にも欠ける。

【0006】一方、最近では、CD-RW（Compact Disc-Rewritable）、MO（MagnetoOptical disc）、D

VD (Digital Versatile Disc) 等に代表される書き換え可能な可搬性の大容量記憶媒体が利用可能になってきている。特に、CD-RWは、媒体価格およびドライブ価格ともに安価で、かつ前世代のCD-ROMも利用可能なことから急速に普及している。

【0007】そこで、このCD-RW等の大容量可搬媒体に各種サービスに専用の端末ソフトウェアを纏めて実装しておき、任意のパーソナルコンピュータに装填されたCD-RW上から直接に任意の端末ソフトウェアを立ち上げることで、パーソナルコンピュータの設置場所に制約されないポータビリティの高いサービスを実現することが考えられる。

【0008】ところが、大容量可搬媒体は、ポータビリティが高いが故に、紛失、盗難等のリスクが常に付きまとい、通常のパスワードによる管理では、本人確認等のセキュリティ管理が不十分となる。このため、電子商取引や、証券、金融サービス等のように高いセキュリティを要求されるサービスには適用が躊躇される。

【0009】このセキュリティ対策として、たとえば、利用者に複雑なパスワードを設定させることが考えられるが、パスワードの暗唱や秘匿等、利用者のパスワード管理負担が大きくなる、という別の技術的課題を生じる。

【0010】本発明の目的は、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【0011】本発明の他の目的は、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【0012】本発明の他の目的は、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用を可能にする可搬性記録媒体およびその使用技術を提供することにある。

【0013】

【課題を解決するための手段】本発明は、アプリケーションソフトウェアが格納される可搬性記録媒体に、指紋等の個人識別情報を予め登録しておき、この個人識別情報を用いた個人認証により、真正のユーザーのみにアプリケーションソフトウェアの利用を可能ならしめるものである。

【0014】すなわち、本発明の可搬性記録媒体は、アプリケーションソフトウェアと、アプリケーションソフトウェアの正当な利用者の個人識別情報と、任意の利用者によるアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行う認証ソフトウェアとが格納されるようにしたものである。

【0015】また、本発明の可搬性記録媒体の使用法

は、アプリケーションソフトウェアが格納された可搬性記録媒体に、アプリケーションソフトウェアの正当な利用者の個人識別情報を格納しておき、任意の利用者による可搬性記録媒体のアプリケーションソフトウェアの使用に先立って個人識別情報を用いた個人認証を行うことで、正当な利用者に、可搬性記録媒体に格納されているアプリケーションソフトウェアを使用させるものである。

【0016】

10 【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【0017】(実施の形態1) 図1は、本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図であり、図2および図3は、本実施の形態の可搬性記録媒体の使用法の一例を示すフローチャートである。

【0018】本実施の形態では、可搬性記録媒体の一例として、CD-RWを例に採って説明する。

【0019】本実施の形態のCD-RW1000は、データの記憶領域が、読み出し専用の物理アクセスプロテクトエリア1001と、書き換え可能なリライタブルエリア1002にて構成されている。

【0020】物理アクセスプロテクトエリア1001は、後述の各種ソフトウェアの書き込み時に、書き換え不能なデータ書き込み方式を用いてデータ書き込みが実行されており、物理的に、書き換え等による改竄が不可能になっている。

【0021】リライタブルエリア1002は、ソフトウェアによる暗号化にて書き込みデータの保護が行われるプロテクトエリア1002-1と、ユーザーや後述のアプリケーションプログラムが自由にアクセス可能なフリーエリア1002-2からなる。

【0022】物理アクセスプロテクトエリア1001には、ユーザー認証プログラム10、指紋認証エンジン20、2フェーズ認証プログラム30、トレーサ40、アプリケーション管理プログラム50、複数のアプリケーションソフトウェア50A、等が格納されている。

【0023】ユーザー認証プログラム10は、後述のように、外部から入力されるユーザーの指紋情報と、予め登録されている指紋情報とに基づいて真正のユーザーを判別する処理を行うソフトウェアであり、ユーザーID管理機能10-1、指紋情報管理機能10-2、認証要求機能10-3等の機能を備えている。

【0024】指紋認証エンジン20は、ユーザー認証プログラム10の配下で指紋情報の照合処理を行うソフトウェアであり、入力された指紋情報および登録されている指紋情報から各々の特徴情報を抽出する指紋データ抽出機能20-1、および特徴情報の照合による一致/不一致の判定を行う指紋照合機能20-2等の機能を備えている。

50 【0025】2フェーズ認証プログラム30は、後述の

ような外部の認証サーバーに指紋照合を依頼する等の認証処理を行うソフトウェアであり、認証サーバー連携機能30-1等を備えている。

【0026】トレーサ40は、指紋による認証プロセスの監視や記録等の処理を行うものであり、後に不正アクセスの解析等を行うべく、たとえば認証が不成功に終わったときに入力された指紋情報等を記録する指紋データ収集機能40-1等を備えている。

【0027】アプリケーション管理プログラム50は、後述の2フェーズ認証プログラム30にて認証サーバー等から得られるライセンスキー等に応じて、各種のアプリケーションソフトウェア50Aの各々について、利用可能な機能等の制限を行うためのアプリケーションライセンスキー管理機能50-1等を備えている。

【0028】アプリケーションソフトウェア50Aとしては、たとえば、銀行との決済取引関連のサービスをサポートするバンキング・トランザクションソフトウェア、投資信託、株式、その他の金融商品の運用管理サービスを行うアセット・マネジメントソフトウェア、保険商品サービスを行うライフ・プランニングソフトウェア、投資関連情報、企業情報、等を提供するフィナンシャル・インフォメーションソフトウェア、電子商取引を行うための電子商取引ソフトウェア、等を格納することができる。

【0029】リライタブルエリア1002のプロテクトエリア1002-1には、ユーザー情報60、指紋情報70、ログ情報80、認証キー情報90、等が格納される。

【0030】ユーザー情報60は、個々のユーザーにユニークに付与されたユーザーID60-1、指紋登録有無フラグ60-2、等の情報からなる。

【0031】指紋情報70は、後述の登録処理にて得られたユーザーID70-1、および指紋データ70-2、等の情報からなる。

【0032】ログ情報80は、指紋認証処理で照合が不成功に終わったときに得られたユーザーID80-1、および指紋データ80-2、図示しない日時データ等の情報からなる。

【0033】認証キー情報90は、ユーザーID90-1、アプリケーションソフトウェア名90-2、ライセンスキー90-3、等の情報からなる。

【0034】図6は、本実施の形態の可搬性記録媒体の利用方法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【0035】図6のパーソナルコンピュータ2000において、2001はマイクロプロセッサ(MPU)、2002はマイクロプロセッサ2001にて実行されるソフトウェアやデータ等が格納される主記憶、2003は、固定ディスク装置(HDD)等の外部記憶装置、2004は、外部から装填されるCD-RW1000に対

するデータの入出力を行うCD-ROMドライブ、CD-RWドライブ等の可搬媒体ドライブ、2005はインターネット等の情報ネットワークに接続されるネットワークインタフェース、2006はユーザーインタフェース、2007は指紋等の個人識別情報を取り込むための個人識別情報入力装置、2008は、これらの各部が接続されるバスである。

【0036】個人識別情報入力装置2007は、たとえば、ユーザーインタフェース2006を構成するディスプレイ、キーボード、マウス等と一体型の装置でもよいし、これらとは独立な装置形態であってもよい。

【0037】主記憶2002には、たとえば、パーソナルコンピュータ用の汎用オペレーティングシステム2002aが常駐し、この汎用オペレーティングシステム2002aの上で、CD-RW1000から当該主記憶2002にロードされる、上述の、アプリケーションソフトウェア50Aが稼働する。

【0038】以下、本実施の形態の可搬性記録媒体およびその使用方法の作用の一例について説明する。なお、図2において括弧付きで記載されている符号は、当該処理を実行するプログラムや機能の符号を示している。

【0039】まず、図2のフローチャート等を参照して、正当なユーザーの指紋情報のCD-RW1000への登録処理について説明する。なお、この登録処理は、たとえば、アプリケーションソフトウェア50A等をCD-RW1000に格納してユーザーに提供する際に、提供者の管理下で正当なユーザーに登録処理を行わせることで、セキュリティが保たれる。

【0040】CD-RW1000のユーザーは、当該CD-RW1000を可搬媒体ドライブ2004に装填することにより、OS2002aの媒体自動起動メカニズムにてCD-RW1000を起動し、ユーザー認証プログラム10、指紋認証エンジン20等を主記憶2002にロードして実行する(ステップS001)。

【0041】なお、CD-RW1000の起動は、OS2002aの媒体自動起動メカニズムを用いて行わせることに限らず、メニュープログラムを立ち上げて、当該メニュープログラムから行わせるようにしてもよい。

【0042】ユーザー認証プログラム10のユーザーID管理機能10-1は、ユーザー情報60の指紋登録有無フラグ60-2を参照して、登録済か否かを判定し(ステップS002)、登録済でない場合は、指紋登録を促す認証情報設定画面をユーザーに提示する(ステップS003)。

【0043】この画面を見たユーザーは、まず、所定の形式のユーザーIDを入力し(ステップS004)、入力された当該ユーザーIDは、ユーザーID管理機能10-1により、ユーザー情報60にユーザーID60-1として書き込まれる(ステップS005)。

【0044】次に、ユーザーは自己の指紋を個人識別情

報入力装置2007にて読み取らせ(ステップS006)、読み取られた指紋情報は、ユーザー認証プログラム10にて起動された指紋認証エンジン20の指紋データ抽出機能20-1にて特徴情報が指紋データとして抽出され(ステップS007)、抽出された指紋データは、指紋情報管理機能10-2による暗号化を経て、ユーザーIDとともに、ユーザーID70-1および指紋データ70-2として指紋情報70に格納され(ステップS008)、指紋データ登録処理が完了する。

【0045】次に、上述のような登録後における任意の契機でのアプリケーションソフトウェアの利用方法の一例について説明する。

【0046】CD-RW1000のユーザーは、当該CD-RW1000を、最寄りのパーソナルコンピュータ2000の可搬媒体ドライブ2004に装填することにより、OS2002aの媒体自動起動メカニズムにてCD-RW1000を起動し、ユーザー認証プログラム10、指紋認証エンジン20等を主記憶2002にロードして実行する(ステップS010)。

【0047】ユーザー認証プログラム10のユーザーID管理機能10-1は、ユーザー情報60の指紋登録有無フラグ60-2を参照して、登録済を確認し(ステップS011)、正当なユーザーか否かを判別するための指紋認証を行うべく、ユーザーに指紋読み取り処理の実行を促す指紋認証画面をユーザーに提示する(ステップS012)。

【0048】この画面を見たユーザーは、個人識別情報入力装置2007から自己の指紋を入力し(ステップS013)、読み取られた指紋から、指紋認証エンジン20の指紋データ抽出機能20-1にて特徴情報が指紋データとして抽出され、同時に指紋データ抽出機能20-1は、指紋情報70から登録されている指紋データ70-2を読み出し(ステップS014)、指紋照合機能20-2にて、入力された指紋データと登録済の指紋データ70-2の一致/不一致の照合判定を行い(ステップS015)、一致すると判定された場合には、ユーザーからの任意のアプリケーションソフトウェア50Aの起動要求を受け付け、利用を許可して(ステップS016)、当該アプリケーションソフトウェア50Aを、CD-RW1000から読み出して起動し、ユーザーに利用させる(ステップS017)。

【0049】起動されたアプリケーションソフトウェア50Aは、稼働に必要なデータおよび稼働中に発生したデータの中でセキュリティ管理必要なデータは、CD-RW1000のプロテクトエリア1002-1の空き領域を利用して暗号化して書き込み、その他のデータは、フリーエリア1002-2を利用して記録する。これにより、CD-RW1000のみで稼働する。

【0050】なお、上述のように単に、アプリケーションソフトウェア50Aを起動して利用させるだけに限ら

ず、たとえば、ユーザー情報60あるいは指紋情報70の一部に、任意のアプリケーションソフトウェア50Aと、ユーザーIDにて特定される特定ユーザー毎のライセンスレベル情報を設定しておき、ステップS016の起動時に、当該アプリケーションソフトウェア50Aにて利用可能な機能に制限を加えることもできる。

【0051】ステップS015で不一致と判定された場合には、入力された指紋データやユーザーID、日時データ等の経過情報をログ情報80に記録する(ステップS018)。このログ情報80を参照することで、当該CD-RW1000の利用経過や、不正使用の追跡、解析等を的確に行うことが可能になる。

【0052】なお、上述の判定処理では、ステップS013～ステップS015、ステップS018を所定の設定回数だけ反復させ、設定回数を超過した場合には、以降の当該CD-RW1000の使用を不能にする処理を加えてもよい。

【0053】このように、本実施の形態のCD-RW1000およびその使用方法によれば、CD-RW1000に予め登録された指紋等の個人識別情報を用いてユーザー認証を行うので、パスワード管理等の負担をユーザーにかけることなく、高い本人同一性の保証が可能となり、高いセキュリティを実現できる。また、可搬媒体であるCD-RW1000にサービス提供に必要なすべてのアプリケーションソフトウェア50Aが格納されているので、CD-RW1000の利点である高いポータビリティと合わせて、CD-RW1000に格納されている多様なアプリケーションソフトウェア50Aの簡便な利用を可能にする効果がある。

【0054】すなわち、CD-RW1000を携帯するユーザーは、最寄りのパーソナルコンピュータ2000にCD-RW1000を装填するだけで、高いセキュリティを必要とする任意のサービスを受けることができる。

【0055】この結果、電子商取引や金融関係等、高いセキュリティを必要とするアプリケーションソフトウェア50Aの格納および利用に、CD-RW1000を安心して利用でき、高いセキュリティおよびポータビリティによるユーザーおよびサービス提供側の利便性の向上を実現できる。

【0056】(実施の形態2)次に、本発明の可搬性記録媒体の使用方法的他の実施の形態について説明する。

【0057】上述の実施の形態1の説明では、CD-RW1000に格納されていたユーザー認証プログラム100等を用いて、当該CD-RW1000にて閉じた状態で認証処理を行う例を説明したが、指紋の照合や認証処理を外部のサーバー等に依頼することで、より多様なアプリケーションソフトウェア50Aの使用における認証管理等を実現することもできる。以下のこのようなCD-RW1000の使用方法的一例について説明する。

20

30

40

50

【0058】図4は、本発明の実施の形態2である可搬性記録媒体の使用法の一例を示すフローチャートであり、図5は、本実施の形態2にて用いられる認証サーバーの構成の一例を示す概念図である。

【0059】なお、実施の形態1と同一の構成要素については同一符号で引用することとし、重複する説明は割愛する。

【0060】まず、図5にて本実施の形態2における認証サーバー3000の構成例について説明する。認証サーバー3000は、制御ソフトウェア3001として、

ユーザー認証プログラム100、指紋認証エンジン200、トレーサー300、アプリケーション利用管理プログラム400、を備えている。

【0061】ユーザー認証プログラム100は、ユーザーID管理機能100-1を備えている。

【0062】指紋認証エンジン200は、指紋照合機能200-1を備えている。

【0063】トレーサー300は、指紋データ収集機能300-1を備えている。

【0064】アプリケーション利用管理プログラム400は、アプリケーション利用可否判定機能400-1、アプリケーション利用ライセンスキー発行管理機能400-2を備えている。

【0065】また、認証サーバー3000は、データベース3002として、ユーザー情報500、ログ情報600、アプリケーション利用情報700、等を備えている。

【0066】ユーザー情報500には、認証サーバー3000の管理者にて登録管理されるユーザーID500-1が記録されている。

【0067】ログ情報600には、指紋認証に失敗した認証処理にて得られたユーザーID600-1、および指紋データ600-2、図示しない日時データ等が記録される。

【0068】アプリケーション利用情報700には、認証サーバー3000の管理者にて登録管理される複数のユーザーID700-1と、当該ユーザーID700-1に対応して利用許可が設定されたアプリケーションソフトウェア50Aのアプリケーションソフトウェア名700-2、当該アプリケーションソフトウェア50Aについて当該ユーザーID700-1のユーザーに許可設定された利用の可否や利用レベル等を示すライセンスキー700-3等が互いに対応付けられて格納されている。

【0069】以下、図4のフローチャートにて、本実施の形態2の作用の一例について説明する。なお、図4において括弧付きで記載されている符号は、当該処理を実行するプログラムや機能の符号を示している。

【0070】CD-RW1000の起動は、上述の実施の形態1の場合と同様であるが、この実施の形態2の場

合には、ユーザー認証プログラム10および2フェーズ認証プログラム30が使用される。そして、サービス選択の図示しないメニュープログラムが起動され、実際の各サービスの入口で、ユーザー認証プログラム10および2フェーズ認証プログラム30にて、認証サーバー3000を利用した指紋認証を行う。

【0071】すなわち、まず、CD-RW1000の起動時の任意のアプリケーションソフトウェア50Aを用いるサービスを選択すると、ユーザー認証プログラム10によるユーザーからのユーザーIDおよび指紋の入力処理が実行され（ステップS020）、ユーザーから入力された指紋データおよび、図2のフローチャートの処理にて予めCD-RW1000に登録されている登録済のユーザーID70-1、指紋データ70-2、当該サービスにて起動されるアプリケーションソフトウェア50Aの名前であるアプリケーションソフトウェア名90-2が、2フェーズ認証プログラム30の認証サーバー連携機能30-1にて、認証サーバー3000に送られる（ステップS021）。

【0072】これを受けた認証サーバー3000は、ユーザー認証プログラム10にて、ユーザーID500-1とユーザーID70-1との照合によるユーザー確認を行った後（ステップS022）、ユーザーから入力された指紋データと、登録済の指紋データ70-2との照合を行う（ステップS023）。

【0073】そして、指紋照合結果が一致しない場合には、ユーザー（パーソナルコンピュータ2000）側から受信した指紋データ等をログ情報600に、日時データ等とともに記録するとともに（ステップS024）、当該サービスの利用不可をユーザーに回答する（ステップS025）。

【0074】指紋照合結果が一致した場合には、ユーザー側から受信したアプリケーションソフトウェア名90-2およびユーザーID70-1をキーとしてアプリケーション利用情報700を参照することで、当該ユーザーによる当該アプリケーションソフトウェア50Aの利用の可否を判定し（ステップS026）、アプリケーション利用情報700に未登録の場合には、利用不可をユーザー側に回答する（ステップS027）。

【0075】アプリケーション利用情報700に登録済の場合は、対応するライセンスキー700-3をアプリケーション利用情報700から読み出し（ステップS028）、ユーザー側のアプリケーションライセンスキー管理機能50-1に送信する（ステップS029）。

【0076】ユーザー側のアプリケーションライセンスキー管理機能50-1は、当該ライセンスキー700-3、ユーザーID70-1、を、CD-RW1000内の認証キー情報90に、ユーザーID90-1、ライセンスキー90-3、としてアプリケーションソフトウェア名90-2と合わせて登録する（ステップS03

10

20

30

40

50

0)。さらに、当該アプリケーションソフトウェア名90-2に対応したアプリケーションソフトウェア50Aの利用を許可して(ステップS031)、CD-RW1000から起動する(ステップS032)。

【0077】ユーザーは起動されたアプリケーションソフトウェア50Aを用いて、たとえば、インターネット4000を経由して、各サービスの提供元の図示しないWebサーバーにアクセスして、所望のサービス提供を受ける(ステップS033)。

【0078】このように本実施の形態2によれば、上述の実施の形態1と同様の効果が得られるとともに、認証サーバー3000側のアプリケーション利用情報700のライセンスキー700-3の設定により、個々のユーザーおよびアプリケーションソフトウェア50A毎に多様な利用レベルを設定することが可能になる。

【0079】また、認証サーバー3000の側にログ情報600が残るので、個々のユーザーに所有されているCD-RW1000の不正使用の解析やセキュリティ管理をより的確に行うことが可能となる。

【0080】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0081】たとえば、個人識別情報としては、指紋に限らず、声紋、容貌、網膜パターン、筆圧、筆跡等、高いレベルで個人識別が可能な情報を用いることができる。

【0082】また、可搬性記録媒体としては、CD-RWに限らず、MO、DVD、等の可搬性記録媒体、さらには、不揮発性の半導体メモリ等でもよい。

【0083】

【発明の効果】本発明の可搬性記録媒体および可搬性記録媒体の使用法によれば、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【0084】本発明の可搬性記録媒体および可搬性記録媒体の使用法によれば、利用者にパスワード管理等の負担をかけることなく、高いポータビリティおよびセキュリティにて多様なアプリケーションソフトウェアの簡便な利用が可能になる、という効果が得られる。

【0085】本発明の可搬性記録媒体および可搬性記録媒体の使用法によれば、高いポータビリティおよびセキュリティにて、多様なライセンスレベルでのアプリケーションソフトウェアの利用が可能になる、という効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施の形態である可搬性記録媒体の構成の一例を示す概念図である。

【図2】本発明の一実施の形態である可搬性記録媒体の使用法の一例を示すフローチャートである。

【図3】本発明の一実施の形態である可搬性記録媒体の使用法の一例を示すフローチャートである。

【図4】本発明の他の実施の形態である可搬性記録媒体の使用法の一例を示すフローチャートである。

【図5】本発明の他の実施の形態である可搬性記録媒体の使用法にて用いられる認証サーバーの構成の一例を示す概念図である。

【図6】本発明の一実施の形態である可搬性記録媒体の利用法にて用いられるパーソナルコンピュータ等の情報処理装置の構成の一例を示す概念図である。

【符号の説明】

10 ユーザー認証プログラム

10-1 ユーザーID管理機能

10-2 指紋情報管理機能

10-3 認証要求機能

20 指紋認証エンジン

20-1 指紋データ抽出機能

20-2 指紋照合機能

30 2フェーズ認証プログラム

30-1 認証サーバー連携機能

40 トレーサー

40-1 指紋データ収集機能

50 アプリケーション管理プログラム

50-1 アプリケーションライセンスキー管理機能

50A アプリケーションソフトウェア

60 ユーザー情報

60-1 ユーザーID

60-2 指紋登録有無フラグ

70 指紋情報

70-1 ユーザーID

70-2 指紋データ

80 ログ情報

80-1 ユーザーID

80-2 指紋データ

90 認証キー情報

90-1 ユーザーID

90-2 アプリケーションソフトウェア名

90-3 ライセンスキー

100 ユーザー認証プログラム

100-1 ユーザーID管理機能

200 指紋認証エンジン

200-1 指紋照合機能

300 トレーサー

300-1 指紋データ収集機能

400 アプリケーション利用管理プログラム

400-1 アプリケーション利用可否判定機能

400-2 アプリケーション利用ライセンスキー発行管理機能

500 ユーザー情報

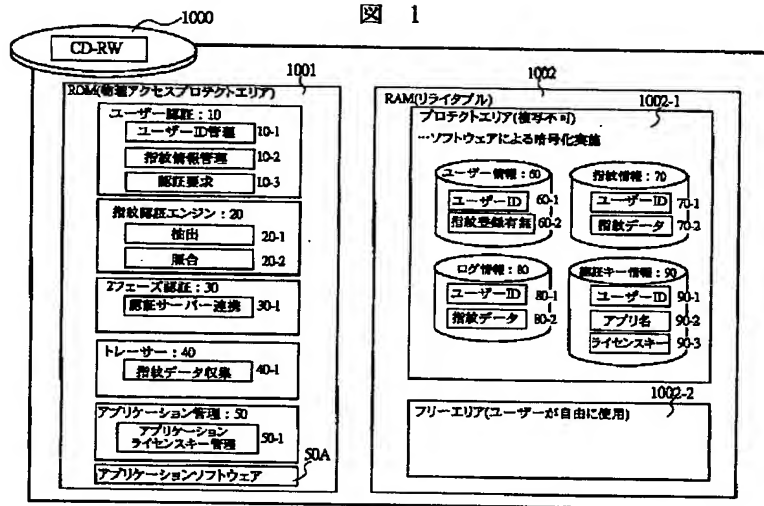
500-1 ユーザーID

600 ログ情報
 600-1 ユーザーID
 600-2 指紋データ
 700 アプリケーション利用情報
 700-1 ユーザーID
 700-2 アプリケーションソフトウェア名
 700-3 ライセンスキー
 1000 CD-RW
 1001 物理アクセスプロテクトエリア
 1002 リライタブルエリア
 1002-1 プロテクトエリア
 1002-2 フリーエリア
 2000 パーソナルコンピュータ

* 2001 マイクロプロセッサ
 2002 主記憶
 2002a 汎用オペレーティングシステム
 2003 外部記憶装置
 2004 可搬媒体ドライブ
 2005 ネットワークインタフェース
 2006 ユーザーインタフェース
 2007 個人識別情報入力装置
 2008 バス
 10 3000 認証サーバー
 3001 制御ソフトウェア
 3002 データベース
 * 4000 インターネット

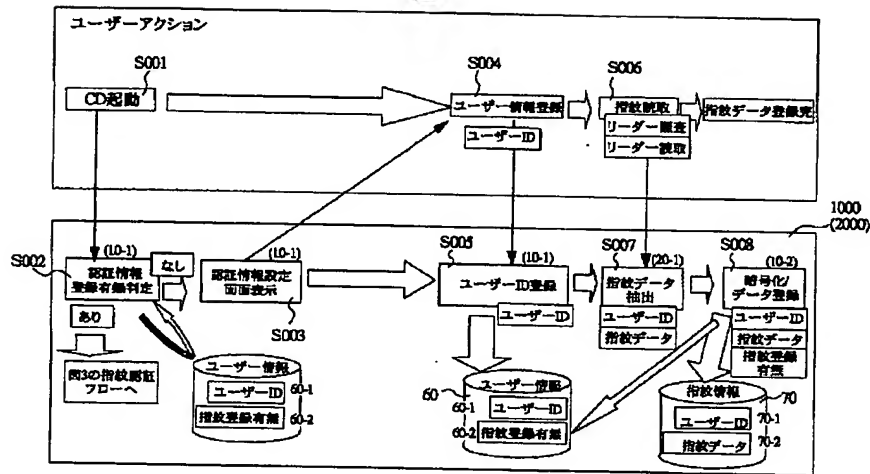
【図1】

図 1



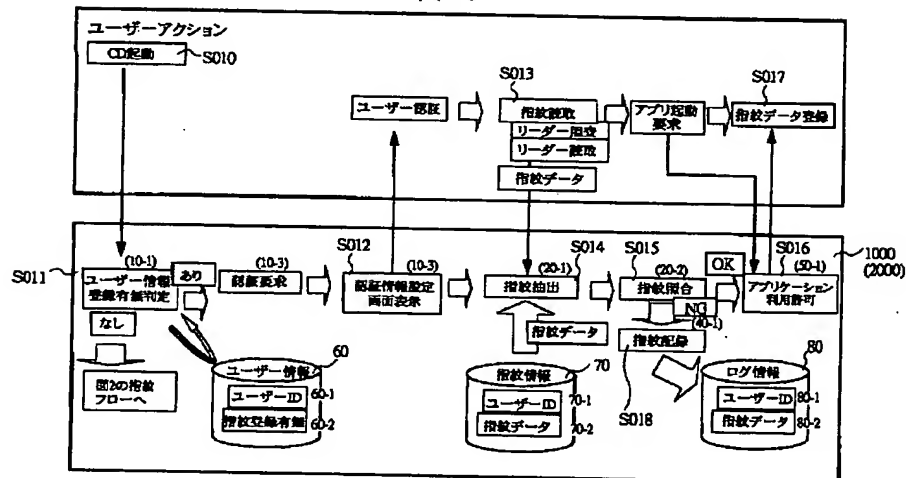
【図2】

図 2

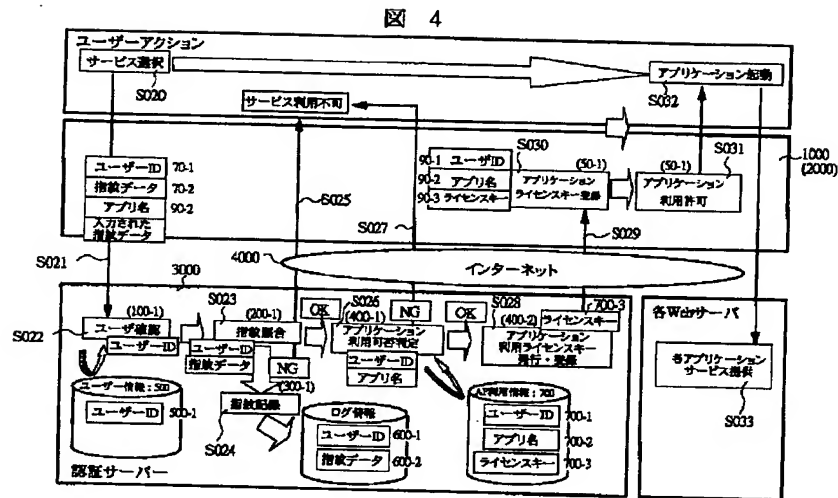


【図3】

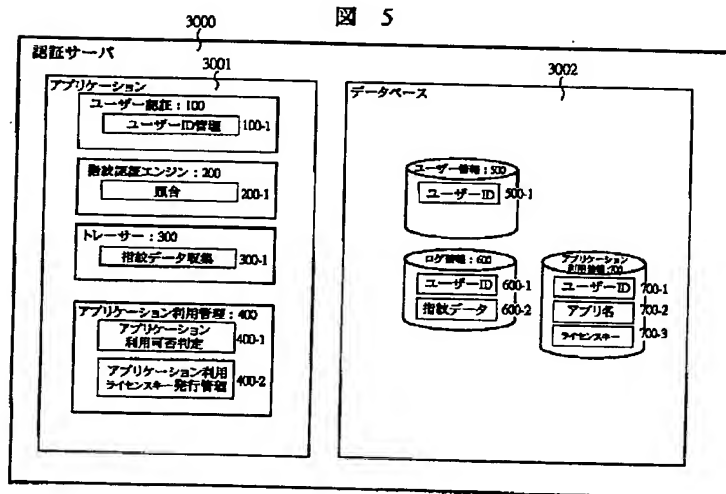
図 3



【図4】

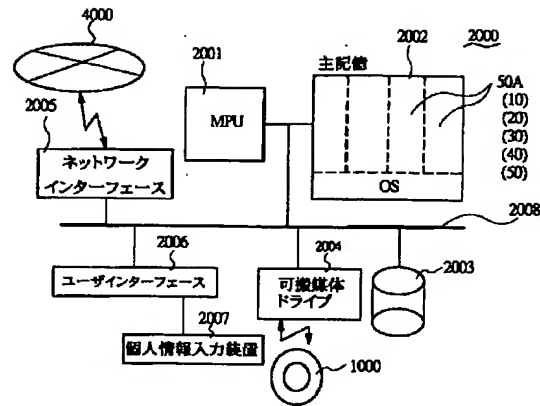


【図5】



【図6】

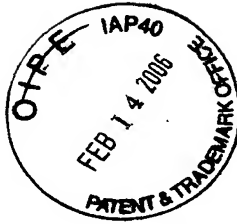
図6



フロントページの続き

(72)発明者 吉田 直邦
東京都新宿区西新宿7-22-45 ベーステ
クノロジー株式会社内

Fターム(参考) 4C038 FF01 FF05 VA07 VB40 VC20
5B076 FB01



THIS PAGE BLANK (USPTO)